Hindawi
Scientific Programming
Volume 2020, Article ID 8848885, 13 pages
https://doi.org/10.1155/2020/8848885

Research Article

Multipurpose Watermarking Algorithm for Medical Images

Shaozhang Xiao, Zhengwei Zhang, Yue Zhang, and Changhui Yu

Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, Huai'an, Jiangsu 223003, China

Correspondence should be addressed to Zhengwei Zhang; zzw49010650@sina.com

Received 1 May 2020; Revised 7 August 2020; Accepted 18 August 2020; Published 1 September 2020

Academic Editor: Manuel E. Acacio Sanchez

Considering the existing medical image watermarking algorithms, a single function often has limitations, and a multipurpose watermarking algorithm for medical images is proposed. First, medical images are divided into regions of interest (ROIs) and regions of noninterest (RONIs). Then, the authentication watermark produced for each subblock of the ROI is embedded into the corresponding mapping subblock. The visible watermark is embedded into the RONI, and, finally, the watermark information and constructed authentication information in each subblock of the ROI are embedded into the corresponding RONI subblock. Simulation results show that the embedded visible watermark can protect and facilitate medical image management. In addition, the proposed algorithm has strong robustness and very good visual quality. It can simultaneously realize copyright protection and content authentication and also has high tamper localization capability.

1. Introduction

In early image watermarking algorithms, a single watermark is embedded into the original image to provide copyright protection [1]. However, with the further development of image watermarking technology, researchers found that embedding a single watermark into the original image for copyright protection and content integrity authentication is not very effective. Its application has some limitations.

Due to the particularity of medical images, medical image information is vulnerable to tampering, illegal copying, patient privacy disclosure, and other information security problems in the network transmission. Therefore, it is necessary to verify the authenticity and integrity of medical image data [2, 3]. Compared with ordinary images, medical images have some unique requirements for watermark embedding: (1) Because of the particularity of medical images, the changes in the image must be very small when embedding watermark; in particular, some key parts (such as lesions) cannot be changed. (2) The information security of the embedded watermark has strict requirements. In particular, the medical records of some special patients are thought to be state and enterprise secrets and should definitely not be disclosed, so illegal extraction of the watermark should be infeasible. (3) Medical records as watermark should be extracted completely and accurately when needed; that is, the embedded watermark should have a certain robustness.

Zhang et al. [4] proposed a dual reversible watermarking algorithm with tamper detection based on multiscale decomposition. The algorithm has high tamper localization ability, but it cannot provide copyright protection. Berchtold et al. [5] proposed using MSERs (maximal stable extremal regions) to extract the ROI to construct a robust watermark. Although the MSERs are used to ensure that the selected region has a certain degree of robustness, this method cannot completely find the exact substantive region for strong protection in medical images. Arsalan et al. [1] proposed using genetic programming (GP) algorithm to embed watermark. The algorithm finds a suitable compression method through GP algorithm, which makes the embedded watermark invisible and has a stable impact on the visual quality when the amount of embedding is increased.

The study in [6] presented a secure multiple watermarking method based on discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD). The proposed method can withstand a variety of signal processing attacks, and the technique is

robust against Checkmark attacks. This algorithm is mainly aimed at robustness and does not have a function of content authentication. At the same time, the algorithm is irreversible, which is not allowed for medical images. To resist geometric attacks, the study in [7] proposed a robust multiwatermarking algorithm suitable for medical images. The proposed algorithm has good performance in terms of robustness and resistance to geometric attacks and conventional attacks, especially in geometric attacks. However, this algorithm is mainly aimed at robustness against attacks and does not have a content authentication function. The above algorithms can only provide a single function, either for copyright protection or for content authentication.

To solve the problem of the limited function of a single watermarking, some researchers proposed embedding two or more watermarks into the carrier image. Ye [8] proposed a dual-function watermarking based on copyright protection and content authentication. The algorithm has high tamper localization accuracy and good visual quality, but its antiattack ability is not strong. A medical image watermarking based on ROI and contourlet transform was proposed in [9]. The algorithm embeds watermark in the background area using the improved difference expansion and selects a greater energy part of the high-order directional subband from the contours of medical images. The authentication watermark is embedded using the comparison algorithm between the direction subband coefficient and 8-neighbourhood mean. The watermark can be blindly extracted, but the tamper localization accuracy and robustness are not high. Literature [10] proposed a dual watermarking algorithm based on the fractional Fourier transform. The algorithm has high location accuracy and strong antiattack ability, but finding a suitable watermark embedding method is difficult.

In [11], a region adaptive dual watermarking algorithm was proposed. Firstly, the carrier image is transformed by integer wavelet transform (IWT), and then the transformed coefficients are divided into different regions. A gray image is embedded in the robust watermark area, and the binary image of the gray watermark is embedded in the fragile watermark area. The algorithm not only realizes the multifunction watermarking but also enhances the robustness of the extracted watermark.

The study in [12] proposed a new fragile watermarking-based scheme for image authentication and self-recovery for medical applications. A host image is broken into 4×4 blocks and SVD is applied by inserting the traces of blockwise SVD into the least significant bit (LSB) of the image pixels to figure out the transformation in the original image. The proposed scheme is tested against different types of attacks such as text removal attack, text insertion attack, and copy and paste attack. Compared with the state-of-the art methods, the proposed scheme greatly improves both tamper localization accuracy and the peak signal-to-noise ratio of self-recovered image.

In [13], the carrier image was transformed by IWT; then, the robust watermark was embedded in the low-frequency subband, and the fragile watermark was embedded in the high-frequency subband. The algorithm has good performance in copyright protection and content authentication. Hurrah et al. [14] proposed a new dual watermarking for copyright protection, data security, and content authentication. The experimental results reveal that the proposed framework offers high degree of robustness against single/dual/triple attacks; the fragile watermark embedding makes the system capable of the tamper detection and localization with average bit error rate (BER) more than 45% for all signal processing/geometric attacks.

In [15], tamper recognition and authenticity were obtained by concealing the dual watermark into the RONI blocks of the medical image. These blocks are chosen by the characteristics of Human Visual System (HVS) with the integration of DWT and Schur transform along with the Particle Swarm Bacterial Foraging Optimization (PSBFO) algorithm. The major focus of the PSBFO is to select the threshold value for obtaining optimum results in terms of imperceptibility and robustness against attacks. Simulation outcomes conducted on different types of medical images disclose that the proposed scheme demonstrates superior transparency and robustness against signal and compression attacks. The study in [16] proposed a watermarking algorithm based on dual fragile watermark: diffusion watermark and authentication watermark. The scrambled authentication watermark and diffusion watermark are arbitrarily embedded into two LSB layers through a random sequence controlled by a secret key. The design aims to enhance the security of fragile watermarking, and the statistical results and security analysis show that this scheme can resist chosen cover-image attacks.

The multipurpose watermarking algorithms proposed by researchers basically involve embedding the invisible watermark but no visible watermark [17], so classifying a large number of watermarked medical images is difficult for hospitals when the medical images only have invisible watermark embedded. Extraction of the watermark for classifying medical images by a special watermarking system every time requires too much work. In this paper, we use image fusion technology to embed a visible watermark, which is equivalent to the signature of the medical image. This indicates that the source of the medical image is official and can be used as the first line of protection and verification for the original medical image.

A multipurpose watermarking with copyright protection and content authentication is proposed instead of an algorithm based on single watermarking or semifragile watermarking [18], which is imperfect for medical images and cannot provide good copyright protection and tamper localization. Because of the characteristics of medical images, completely restoring the ROI when the watermark is extracted is necessary. Therefore, a reversible image watermarking is used to embed watermark in ROI. Thus, in this paper, a triple watermarking algorithm based on IWT, general difference extension, and image fusion is studied.

2. Related Theory

2.1. Medical Image Segmentation. The ROI usually refers to the region in medical images with large pixels and complicated textures, while the RONI usually refers to continuous black regions.

Edge detection is the most basic treatment for all edge-based segmentation methods. The Laplacian operator [19, 20] is a second-order differential operator independent of the edge direction and is linear and rotational invariant. For a continuous function $f(x, y)$, its Laplacian operator expression at position (x, y) is

$$\nabla^2 f(x,y) = \frac{\partial^2 f(x,y)}{\partial x^2} + \frac{\partial^2 f(x,y)}{\partial y^2}, \tag{1}$$

$$G(i,j) = |4f(i,j) - f(i+1,j) - f(i-1,j) - f(i,j+1) - f(i,j-1)|.$$

After edge detection, the medical image can be segmented using the level set, which is first introduced by Osher and Sethian [21]. The basic idea is not to operate on the contour directly but to set the n-dimensional contour as the $(n+1$-dimensional) zero-level set of a higher-dimensional function. This higher-dimensional function is called the level set function $\varphi(X,t)$. At time t, the motion contour can be obtained by extracting the zero-level set $c((X),t) = \{\varphi(X,t) = 0\}$ from the differential equation.

In the two-dimensional case for example, the level set method views the closed curve $C(t)$ in the two-dimensional plane as the $\{\varphi = 0\}$ zero-level plane in the continuous function surface φ in the three-dimensional space; namely,

$$C(t) = \{(x,y) \mid \varphi(x,y,t) = 0\}, \tag{2}$$

where t represents time. Take the partial derivative with respect to time on both sides of the following equation:

$$\frac{\theta\varphi}{\theta t} + \frac{\theta\varphi}{\theta x}\cdot\frac{\theta x}{\theta t} + \frac{\theta\varphi}{\theta y}\cdot\frac{\theta y}{\theta t} = 0. \tag{3}$$

To solve this equation, assume that the movement speed function in the normal direction of the surface is $F(x, y)$:

$$F(x,y) = \left[\frac{\theta x}{\theta t}, \frac{\theta y}{\theta t}\right]\cdot n, \tag{4}$$

where n is the unit normal vector:

$$n = -\frac{\nabla\varphi}{|\nabla\varphi|}, \qquad \nabla\varphi = \left[\frac{\nabla\varphi}{\nabla x}, \frac{\nabla\varphi}{\nabla y}\right], \tag{5}$$

where $\nabla\varphi$ is the gradient φ of the two-dimensional plane; then,

$$\left[\frac{\theta x}{\theta t}, \frac{\theta y}{\theta t}\right]\cdot\left[\frac{\theta\varphi}{\theta x}, \frac{\theta\varphi}{\theta y}\right] = -F|\nabla\varphi|. \tag{6}$$

Hence,

$$\frac{\theta\varphi}{\theta t} = F|\nabla\varphi|. \tag{7}$$

This equation is the level set equation. Finally, to solve the problem of curve evolution, solve equation (7), where the initial condition is

$$\varphi(x,y,t=0) = \pm d(x,y). \tag{8}$$

In equation (8), $d(x, y)$ is the signed distance function, signifying the shortest distance from pixel (x, y) to closed curve $C(t)$. The sign is determined according to the position of the pixel. If the pixel falls outside of the closed curve, then the sign is positive; otherwise, the sign is negative. At any moment, the points on the curve are the set of points for which the distance function value is 0, which is the zero-level set.

Finally, the image segmentation contour is acquired based on the zero-level set on the level set function surface.

The original image (Figure 1) is first subjected to Laplacian edge detection (Figure 2), and then we obtain a better contour by conducting the level set segmentation (Figure 3).

2.2. Image Fusion. Two images with different types of properties can be fused into one image by image fusion [22]. Three kinds of image fusion techniques can be utilized: pixel-level fusion, feature-level fusion, and decision-level fusion. More information from the original two images is retained with pixel-level fusion, whose accuracy is higher. Therefore, the pixel-level fusion is used to embed the visible watermark into the carrier image in this paper.

I is the original image, and w is the visible watermark. Visible watermark embedding is the fusion of the local region of the image so that a visible watermark image F can be obtained:

$$F_{i,j} = \left(m_I I_{i,j} + m_W W_{i,j}\right). \tag{9}$$

In equation (9), m_I and m_W are the multiplication factors of I and W, where $m_I + m_W = 1$.

The process of eliminating the visible watermark is the inverse of the image fusion process described above, and the carrier image I is recovered from image F:

$$I_{i,j} = \frac{\left(F_{i,j} - m_W W_{i,j}\right)}{m_I}. \tag{10}$$

To ensure the visibility of the visible watermark, when the multiplication factors are selected, they can be increased or decreased as much as possible to obtain better results.

In this paper, a greyscale image of size 512×512 is used as the original image I (Figure 4), and a greyscale image of size 48×24 is used as the visible watermark W_1 (Figure 5).

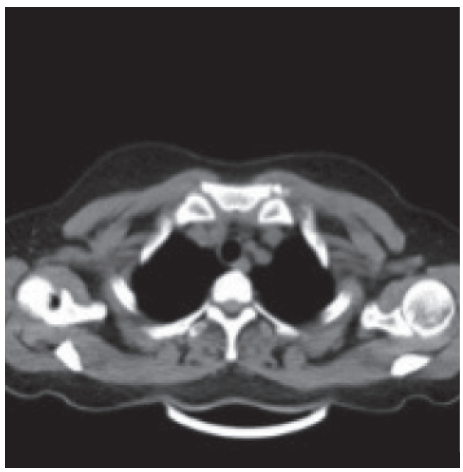


Figure 1: Original image.

Figure 2: Image generated by Laplacian edge detection.

Figure 3: Contour of Figure 2 extracted by level set.

Images with a visible watermark (Figure 6) can be obtained by embedding W_1 in the upper left area of the image I with the same size according to equation (9).

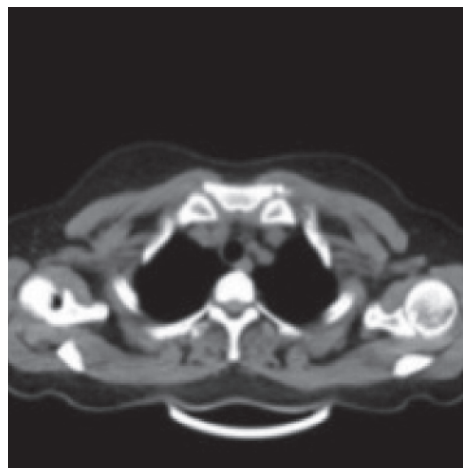


Figure 4: Original image.

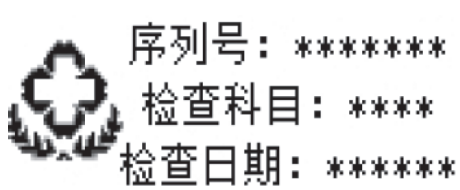


Figure 5: Visible watermark.

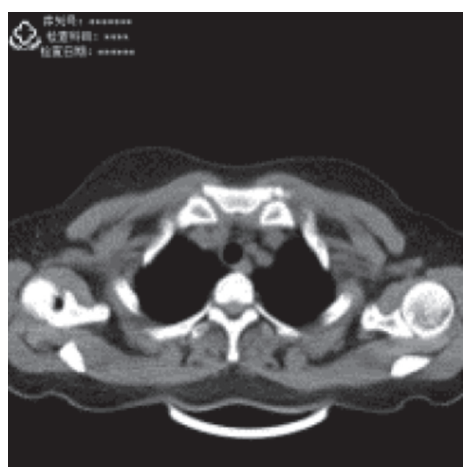


Figure 6: Image with a visible watermark.

3. Algorithm Design

The algorithm in this paper is composed of three modules: watermark generation, watermark embedding, and watermark extraction and tamper localization.

3.1. Authentication Watermark Generation. The singular value [23] of the image has good stability, so its singular value will not greatly change when the image is slightly disturbed. Therefore, the authentication watermark embedded by this algorithm is generated by extracting singular values of image blocks.

Each subblock I_p of the ROI segmented by the Laplacian edge detection and level set method is subjected to SVD; namely, $I_p = U_p S_p V_p^T$.

Its norm is as follows:

$$\mathrm{Cou}_p = \sqrt{\sum_{i=1}^{n} \left(\sigma_p^i\right)^2}, \tag{11}$$

where σ_p^i is the i-th singular value of subblock I_p. Equation (12) is used to calculate the ratio between the maximum singular value σ_p^i and the norm Cou_p of each subblock I_p:

$$k_{p1} = \frac{\sigma_p^1}{\mathrm{Cou}_p}, \tag{12}$$

where k_{p1} is used as the logistic chaotic map [24], the range of k_{p1} is within (0, 1), and the range of logistic map is within (−1, 1). We choose $k_{p2} = k_{p1} - 1$ as the second key to expanding the key space. The key is finally $k_p = k_{p2} + k_{p1}$. Taking k_p as the initial value, a real-valued chaotic sequence $x_p^i, i \in \{1, 2, 3, 4\}$ of 4 in length is generated. Since the mean value of the sequence generated is zero, zero is selected as the threshold for the binarization of x_p^i, where $w_p^i = (\mathrm{sgn}(x_p^i) + 1)/2$, $i \in \{1, 2, 3, 4\}$, and $\mathrm{sgn}(\cdot)$ is a symbolic function that completes the process of authentication watermark generation. The authentication watermark generated in each subblock of the ROI is represented by a 4-bit binary number.

3.2. Watermark Embedding. The process of watermark embedding in the medical image is shown in Figure 7, which includes visible watermark embedding, robust watermark embedding, and authentication watermark embedding. First, the medical image is segmented using the Laplacian edge detection and level sets and divided into ROI I_1 and RONI I_2. To reduce the amount of embedded edge information and improve the invisibility of the algorithm, the segmented image is corrected, and the image is divided into 8×8 blocks. Subblocks at the boundary line are incorporated into the ROI of the image. After that, the visible watermark is embedded in the RONI I_2 by the image fusion algorithm. Then, the robust watermark information and the authentication watermark information generated by ROI I_1 are embedded in RONI I_2 with the embedded visible watermark. Finally, the self-generated authentication watermark information is embedded in ROI I_1 to complete watermark information embedding.

3.2.1. Visible Watermark Embedding. A coordinate is set in RONI I_2 as the visible watermark embedding position (its top left corner (0, 0) is usually selected as the starting position for embedding).

The visible watermark information mainly includes the hospital logo icon, the serial number of the computed tomography (CT) image, the type of examination subject, and the examination time. The inspection time automatically generated by the system and other information included in the visible watermark information is embedded in RONI I_2 using equation (9).

3.2.2. Robust Watermark Embedding

Step 1. Arnold transform is used to scramble the robust watermark information W that needs to be embedded, and the scrambled image is transformed into a one-dimensional vector.

Step 2. After the two-level IWT is applied on each subblock of RONI I_2 (as shown in Figure 8), the four subband coefficients of HL1, LH1, HL2, and LH2 are carried out by SVD.

Step 3. The authentication watermark for each subblock in ROI I_1 is generated by SVD and logistic chaotic mapping.

Step 4. A mapping function between ROI subblocks and RONI subblocks is established by logistic chaotic mapping based on key KI1. Since most of the regions in medical CT images are ROIs, the embedding space of the RONI may be insufficient if the authentication watermark of ROI subblocks is one-to-one embedded in each subblock of the RONI. Therefore, in this paper, the subblocks of the RONI and ROI are sorted from left to right and from top to bottom, and two consecutive subblocks in the ROI are mapped to each subblock of the RONI as a large block (Figure 9). The watermark information after scrambling is divided and integrated according to the number of RONI subblocks, and the authentication watermark mapped to the current subblock of the RONI is embedded as a robust watermark.

Assume that the relationship between a ROI subblock and a RONI subblock is established by a logistic chaotic map, as shown in Figure 9. The 4-bit binary authentication watermark information generated by two subblocks in each large subblock of the ROI is operated by XOR, and the 4-bit binary information generated by XOR is regarded as the authentication watermark generated by each block and embedded in the corresponding subblock of the RONI. If the authentication watermark generated by ROI subblock 3 is 1011 and the authentication watermark generated by subblock 4 is 1001, then the authentication watermark information embedded in RONI subblock 4 is 0010.

Step 5. A new singular value of the IWT coefficient is obtained by embedding watermark using an odd-even quantization. The first singular value and the remaining singular value of the diagonal matrix of each of the subblocks HL1, LH1, HL2, and LH2 in the RONI are sequentially taken, compared, and judged to embed a watermark. An 8-bit binary watermark can be embedded using the four subband coefficients of HL1, LH1, HL2, and LH2.

When $\lfloor \alpha s_i(j, j)/s_i(1, 1) \rfloor$ is even,

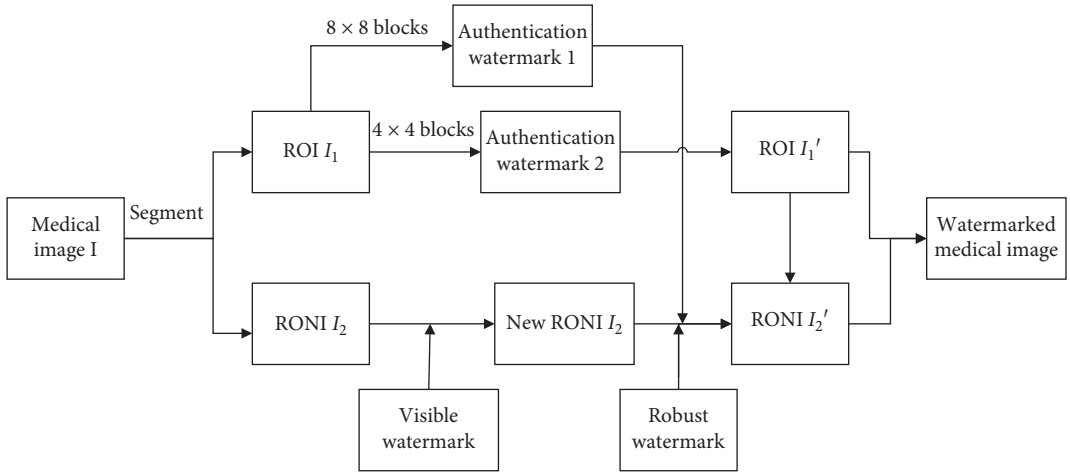


Figure 7: The flowchart of medical image watermark embedding.

Figure 8: Two-layer wavelet decomposition.

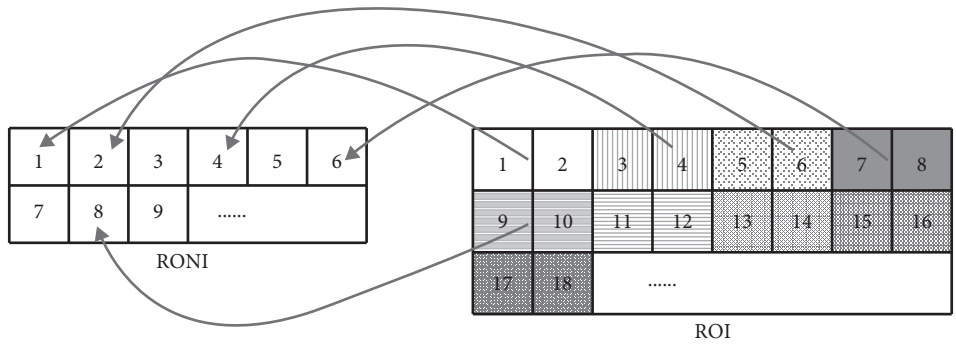


Figure 9: Mapping the relationship between the ROI and RONI.

$$s_{ij} = \begin{cases} s_i(1,1)\left(\left\lfloor \dfrac{\alpha s_i(j,j)}{s_i(1,1)} \right\rfloor + 1\right), & W_i = 1, \\ s_i(1,1)\left(\left\lfloor \dfrac{\alpha s_i(j,j)}{s_i(1,1)} \right\rfloor\right), & W_i = 0. \end{cases} \tag{13}$$

When $\lfloor \alpha s_i(j,j)/s_i(1,1) \rfloor$ is odd,

$$s_{ij} = \begin{cases} s_i(1,1)\left(\left\lfloor \dfrac{\alpha s_i(j,j)}{s_i(1,1)} \right\rfloor\right), & W_i = 1, \\ s_i(1,1)\left(\left\lfloor \dfrac{\alpha s_i(j,j)}{s_i(1,1)} \right\rfloor + 1\right), & W_i = 0, \end{cases} \tag{14}$$

where $\lfloor \rfloor$ is the floor function, W_i is the watermark information, α is the embedding adjustment coefficient, S_{ij} is the j-th singular value of the i-th subblock, and $2 \le j \le 15$.

Step 6. RONI $I_2^{`}$ with watermark information is generated by inverse SVD and inverse 2-layer IWT, combining ROI I_1 with the watermark image with robust watermark information and authentication watermark information is obtained.

3.2.3. Authentication Watermark Embedding

Step 1. ROI I_1 is redivided into 4×4 nonoverlapping blocks, and the authentication watermark is generated

in each subblock of I_1 by SVD and logistic chaotic mapping.

Step 2. The overflow map is constructed. Since the difference expansion is used, the embedding information will go beyond the pixels in the image gray value range, and the overflow map is labelled. The compressed overflow map and authentication watermark are embedded in the corresponding mapping blocks through the generalized difference expansion mode. In this algorithm, the authentication watermark generated by the smooth block is embedded into the corresponding smooth block based on the generalized difference expansion algorithm [25]. Each smooth block is embedded with a 15-bit watermark, wherein the authentication watermark occupies 4 bits, and the remaining bits are used to store overflow map information and related auxiliary information.

Step 3. Based on key KI2, a mapping function for the ROI I_1 subblocks is established by logistic chaotic mapping. The watermark authentication information generated by its block is embedded in the corresponding mapping block, and the logistic chaotic mapping key KI2 is saved for the watermark information extraction and detection.

Step 4. The authentication watermark and other information are embedded into the corresponding subblocks of ROI I_1 by general difference expansion to generate a new ROI I_1'.

Step 5. The final watermarked medical image is obtained by combining ROI I_1' and generated RONI I_2'.

3.3. Watermark Extraction and Tamper Localization. The flowchart of watermark extraction and tamper localization for watermarked medical images in this paper is shown in Figure 10. The specific steps are as follows.

3.3.1. Watermark Extraction. Watermark extraction is mainly the extraction of robust watermark information, and the visible watermark does not need to be extracted. The specific operation is as follows:

Step 1. According to the method of robust watermark embedding, the watermarked medical image is segmented by the Laplacian edge detection and level set method.

Step 2. The segmented image is divided into 8×8 blocks. Subblocks at the boundary line are incorporated into the image ROI, and the image is divided into ROI I_1 and RONI I_2.

Step 3. After the two-layer IWT is applied on every subblock of RONI I_2, the four coefficients of HL1, LH1, HL2, and LH2 obtained by the transform are carried out by SVD.

Step 4. The first value of each diagonal matrix is removed in turn to judge and extract the watermark. If the value of $\lfloor \alpha s_i(j, j)/s_i(1, 1) \rfloor$ is close to an even number, then the watermark information 0 is extracted; if the value is close to an odd number, then the watermark information 1 is extracted. The watermark information in each subblock is extracted by this method.

Step 5. The authentication watermark incorporated into the watermark information is removed, and then the original robust watermark is restored by the Arnold scrambling inverse transform.

3.3.2. Tamper Localization. Medical images require the image to be authentic and complete, and any changes cannot cause image distortion, especially to the ROI in the image. Therefore, the watermark image should be authenticated to determine whether it has been tampered with:

Step 1. The medical image is segmented using the Laplacian edge detection and level sets and divided into ROI I_1 and RONI I_2.

Step 2. RONI I_2 is divided into nonoverlapping subblocks of size 8×8. The authentication watermark contained in the robust watermark information in each subblock is extracted by the above watermark extraction algorithm.

Step 3. ROI I_1 is divided into 4×4 nonoverlapping subblocks; each block is operated on by inverse general difference expansion, and the authentication watermark hidden in the subblock is obtained.

Step 4. The authentication watermark information is extracted from each subblock of ROI I_1, and the feature watermark of each subblock is generated by SVD and logistic mapping.

Step 5. Based on the key KI2, the corresponding mapping subblock for each small block in ROI I_1 is found by logistic mapping, and the feature watermark is compared with the authentication watermark extracted from the mapping subblock. If the values of the authentication watermark in the two subblocks are equal, then the watermark has not been tampered with; otherwise, the watermark has been tampered with, and the tampered region needs to be located.

Step 6. ROI I_1 is redivided into 8×8 nonoverlapping blocks. The corresponding subblocks of RONI I_2 for the ROI I_1 subblocks are found by logistic chaotic mapping based on key KI1. In this paper, each subblock of the RONI and ROI is sorted in order from left to right and from top to bottom, respectively, and two consecutive subblocks in the ROI are mapped into each subblock of the RONI as a large block. For the ROI that has not been tampered with, according to Step 5, the subblock authentication watermark is extracted and compared with the corresponding authentication watermark hidden in each subblock of RONI I_2. If the values are equal, then the watermark has not been tampered with; otherwise, the watermark has been tampered with, and the tampered region needs to be located.

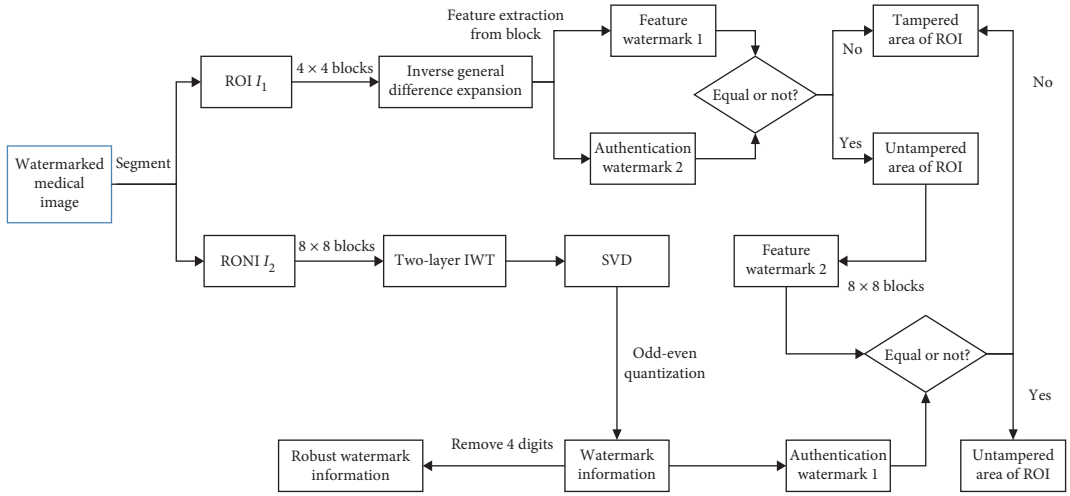


Figure 10: The flowchart of watermark extraction and tamper localization for watermarked medical image.

4. Experimental Results and Analysis

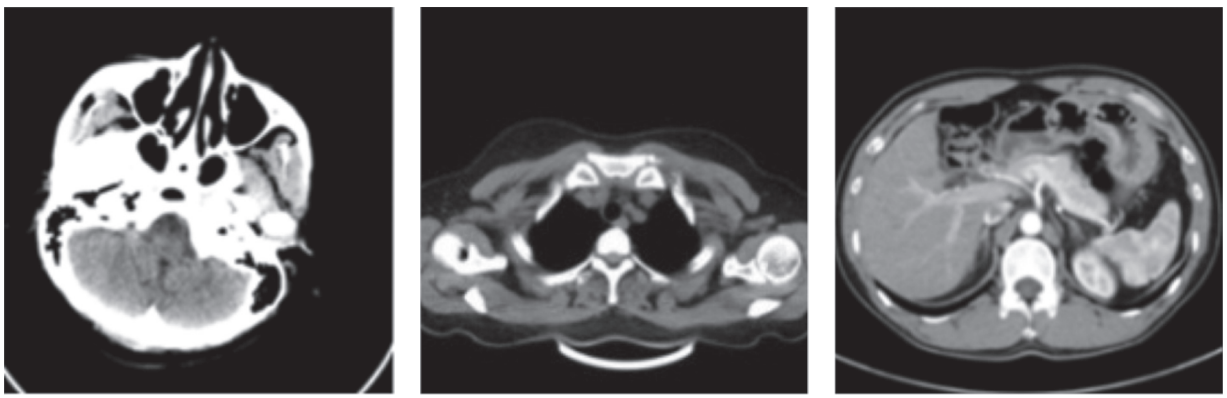
In this experiment, the standard images of the skull, mediastinum, and liver, the size of which is 512×512 and 8-bit greyscale, are randomly selected as the original medical images. All images are from the data centre of Suzhou University Affiliated Hospital. Due to limited space, this article takes three images as examples, as shown in Figure 11. The visible watermark to be embedded is composed of medical image identification and basic information, and the robust watermark is composed of basic patient information and diagnostic information (Figure 12). The experiment focuses on the reversibility of the algorithm, the visual quality of the watermarked image, the accuracy of tamper detection, and the accuracy of regional positioning. All the experiments in this paper are based on MATLAB R2012b in the Windows XP operating system. Image fusion theory was used to embed visible watermark, which is equivalent to adding digital signatures to carrier images. Only on the basis of the digital signature (visible watermark) can the receiver extract the invisible watermark by using the key. Therefore, the analysis of the experimental results in this paper is based on medical images with visible watermark as the carrier images.

When the watermarked medical image is not attacked or tampered with, the ROI recovered by extracting the authentication watermark embedded in the ROI using the watermark extraction algorithm is exactly the same as the original ROI. That is, $I_1(x, y) - I_1'(x, y) = 0$. (x, y) indicates the position of the image pixels in the image, I_1 represents the ROI before the watermark is embedded, and I_1' represents the recovered ROI. Thus, the reversibility of the algorithm is verified.

In this paper, the medical image with a visible watermark, as shown in Figure 13, is used as the carrier image, and basic information, such as the binary image shown in Figure 12(b), is selected as the watermark information. Figure 14 shows the experimental results of watermark embedding and extraction without attack. Through observation by the human eye, image distortion cannot be perceived. In this paper, the peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) are used as measures of the embedding distortion, and the normalized correlation (NC) is used as a measure of the watermarking robustness. Figures 14(a)–14(c) show the watermarked images obtained (including embedded robust watermark and authentication watermark) by this algorithm whose PSNR values are 37.5 dB, 38.57 dB, and 36.21 dB, and SSIM values are 0.985, 0.987, and 0.982, indicating that the algorithm has low distortion and good visual quality. The details are shown in Table 1. Figures 14(d)–14(f) show the three watermark images extracted by this algorithm whose NC values are all 1, which shows that the algorithm can extract the watermark completely without being attacked or tampered with.

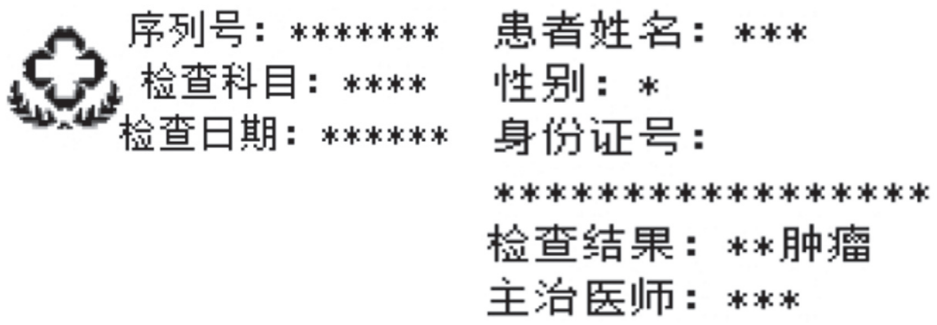
Form Table 1, compared with the algorithms in [1, 14, 26], the visual quality of the proposed algorithm is higher than those of [14, 26] but slightly lower than that of [1]. The visual quality of this algorithm is slightly lower than that of [1]. The main reason is that both robust watermark and authentication watermark are embedded in this algorithm, while only a single watermark is embedded in the algorithm in [1]. Both robust watermark and authentication watermark are embedded in this algorithm and the algorithms in [14, 26], but the PSNR and SSIM values generated by this algorithm are significantly higher than those generated by the algorithms in [14, 26].

When the proposed algorithm is used to embed the watermark in the RONI, not only is the robust watermark embedded but also the authentication watermark is embedded, which makes the embedding capacity slightly larger. The RONI in medical images is smooth, so blocking artefacts can be easily caused after embedding too much information, which leads to a decrease in the image quality. The PSNR values of the three watermarked images after embedding the robust watermark in the RONI are only 40.55 dB, 41.61 dB, and 39.73 dB. The visual quality exhibits little difference compared with that when embedding both the robust watermark and the authentication watermark in the RONI. To



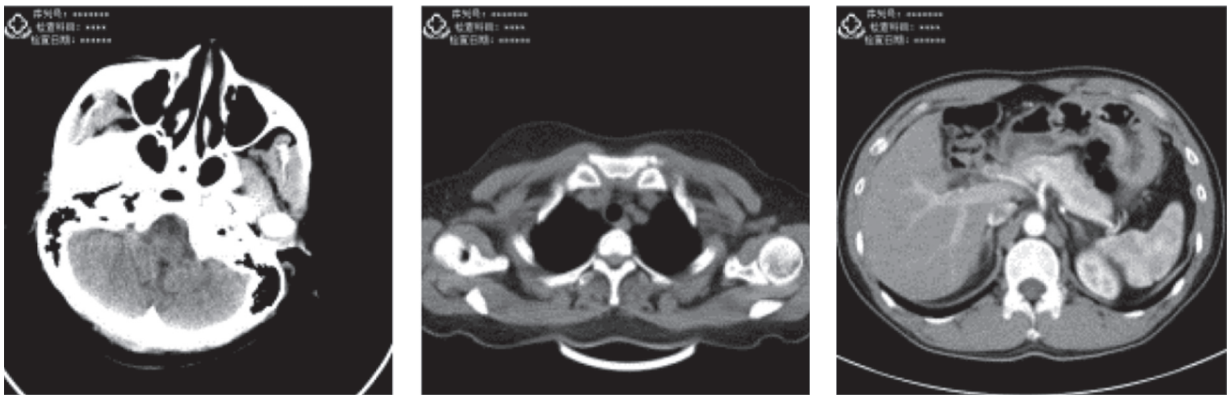
(a) (b) (c)

Figure 11: Original medical images. (a) Skull. (b) Mediastinum. (c) Liver.



(a) (b)

Figure 12: Watermark information. (a) Visible watermark. (b) Robust watermark.



(a) (b) (c)

Figure 13: Images with a visible watermark. (a) Skull. (b) Mediastinum. (c) Liver.

improve the accuracy of tamper localization, reducing the visual quality slightly is worthwhile.

Since the visible watermark is visible to the human eye, an attack on a visible watermark may be a shear attack or an elimination attack. Since the invisible watermark (robust watermark and authentication watermark) is invisible to the human eye, an attack on it may be a JPEG compression attack, a noise attack, a rotation attack, etc. In this paper, a robust watermark is embedded into the RONI for copyright protection and has no impact on medical diagnosis. A

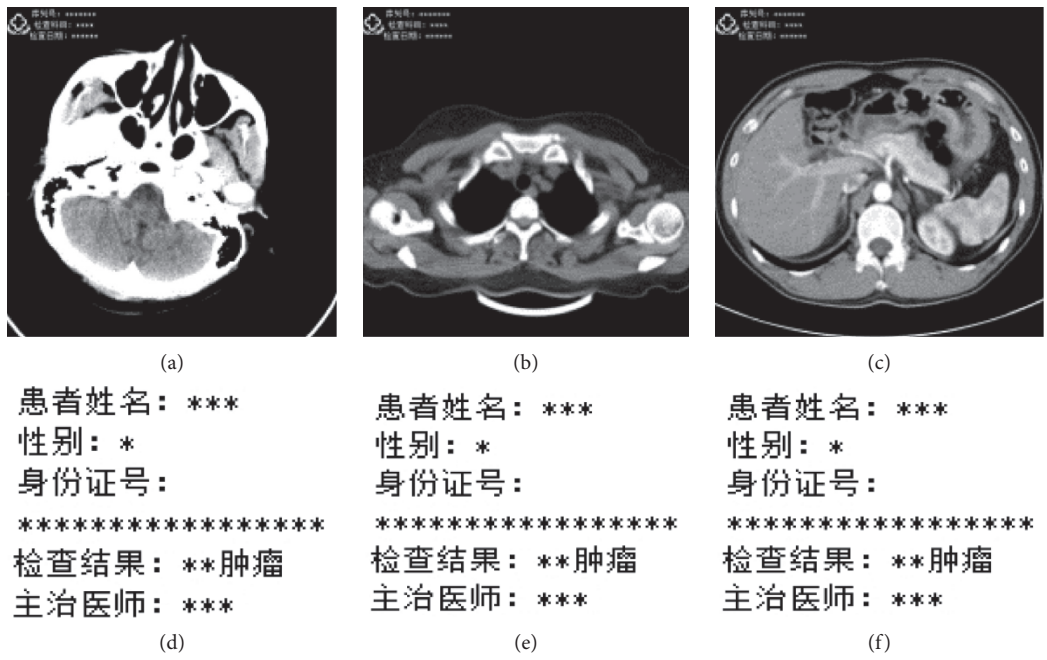


Figure 14: Experimental results of watermark embedding and extracting without attack.

Table 1: Comparison of PSNR (dB) and SSIM.

Image name	Proposed algorithm		Literature [1]		Literature [14]		Literature [26]	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Skull	37.5	0.985	43.72	0.989	34.27	0.981	31.21	0.953
Mediastinum	38.57	0.987	44.37	0.989	36.74	0.982	32.52	0.960
Liver	36.21	0.982	42.94	0.987	34.78	0.981	30.63	0.945

variety of attacks are applied to the three visible watermarked images shown in Figure 13 after embedding the robust watermark shown in Figure 12(b) to compare the robustness (as shown in Table 2). Many kinds of attacks are included in this paper. To verify the antiattack robustness, the use of experimental data from other studies as a reference is necessary. Because the focus of each paper is different, the experimental data it contains may be insufficient; thus, this paper draws on the data from [14, 26–28] for comparison.

The experimental results in Table 2 show that the proposed algorithm has higher robustness than the other algorithms in [14, 26–28]. The "—" in Table 2 indicates that the corresponding experimental measurement has not been carried out. IWT has an excellent effect in gathering energy and is very robust against noise, filtering, and other removal attacks. By using two-layer IWT on the image to obtain more concentrated energy, the robustness can be improved effectively. In addition, the image singular value has good stability, and it is particularly robust against rotation attacks. The paper selects the NC value of the other algorithms that have better resistance to some attacks as the NC value of the whole other algorithms, but, overall, this algorithm has high robustness against attacks on the basis of high invisibility.

Compared with the other algorithms in [14, 26–28], the algorithm in this paper is less robust to some attacks, mainly because the other algorithms are composed of multiple algorithms, and some algorithms are more robust to certain attacks. Although under certain attacks, the robustness of the proposed algorithm is lower than that of some algorithms in [14, 26–28]; on the whole, the antiattack ability of the algorithm in this paper is stronger than any algorithm in [14, 26–28].

In this paper, both robust and authentication watermarks are embedded in the same carrier image (such as Figure 13). Therefore, not only the impact of various attacks on robustness but also the impact of the embedded authentication watermark on robustness should be considered. In Table 3, only a robust watermark is embedded in Algorithm 1, and a robust watermark and an authentication watermark are embedded and authenticated in Algorithm 2.

The watermarked image (Figure 15(a)) is tampered with, and the tampered image is as shown in Figure 15(b). The tampered image is subjected to tamper detection. The detection result is shown in Figure 15(c), and the position of the tampered region is marked in white. Figure 15(d) shows the position matrix of the located tampered region. The position of the tampered region is marked in white, and the position of the other areas is marked in black.

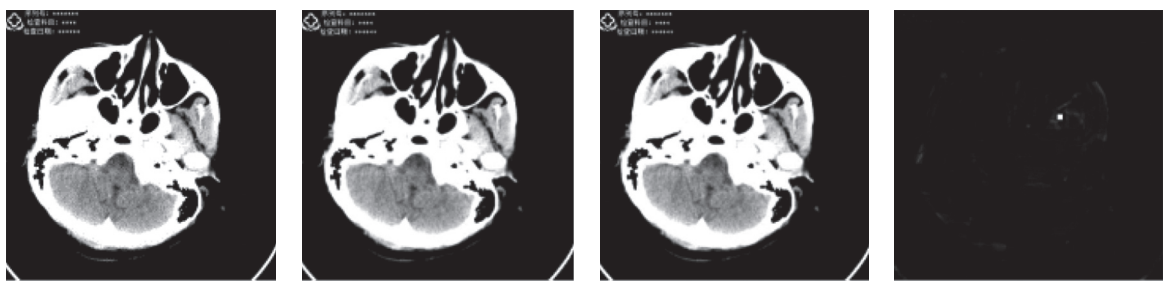
Similarly, the liver image with an embedded authentication watermark is tampered with in the experiment, as shown in Figure 16(b). The tamper detection effect is shown in Figure 16(c), and the position of the tampered region is

Table 2: Similarity of watermark extracted under various attacks.

Attack types	Similarity of robust watermark (NC)														
	Skull					Mediastinum					Liver				
	This paper	[14]	[27]	[26]	[28]	This paper	[14]	[27]	[26]	[28]	This paper	[14]	[27]	[26]	[28]
No attack	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Gaussian filter (3×3 $\sigma = 0.3$)	0.956	—	0.979	—	0.971	0.954	—	0.977	—	0.967	0.944	—	0.972	—	0.959
Median filter [3, 3]	0.942	0.956	0.987	0.861	0.983	0.938	0.951	0.985	0.856	0.982	0.926	0.944	0.982	0.847	0.98
White noise (0.01)	0.961	—	—	0.970	0.958	0.959	—	—	0.969	0.956	0.951	—	—	0.963	0.949
Salt and pepper noise (0.02)	0.957	0.940	0.949	0.946	0.942	0.961	0.942	0.947	0.944	0.940	0.952	0.935	0.942	0.938	0.937
Shear (1/16)	0.921	0.852	—	0.935	0.941	0.920	0.863	—	0.931	0.933	0.906	0.842	—	0.920	0.922
JPEG compression $Q = 20$	0.914	—	—	—	0.743	0.934	—	—	—	0.755	0.921	—	—	—	0.728
JPEG compression $Q = 50$	0.955	—	0.872	0.822	0.857	0.952	—	0.883	0.820	0.870	0.943	—	0.865	0.809	0.854
Shrink 30%	0.982	0.977	—	0.861	1	0.985	0.978	—	0.858	1	0.976	0.971	—	0.857	1
Enlarge 30%	0.985	0.971	—	0.853	1	0.988	0.973	—	0.855	1	0.981	0.968	—	0.849	1
Rotate 30°C	0.983	—	—	0.892	0.975	0.978	—	—	0.888	0.974	0.972	—	—	0.883	0.972
Rotate 45°C	0.976	0.967	—	—	0.964	0.972	0.965	—	—	0.963	0.970	0.961	—	—	0.959

Table 3: Similarity of the extracted watermark based on two algorithms.

Attacking mode	Robust watermark similarity (NC)	
	Algorithm 1	Algorithm 2
No attack	1	1
Gaussian low-pass filter	0.938	0.937
Median filter [3, 3]	0.942	0.943
Gaussian noise (0.05)	0.952	0.949
Salt and pepper noise (0.03)	0.957	0.956
Shear (1/16)	0.921	0.921
JPEG compression $Q = 20$	0.924	0.922
JPEG compression $Q = 50$	0.965	0.964
Shrink 10%	0.985	0.985
Rotate 30°C	0.982	0.982



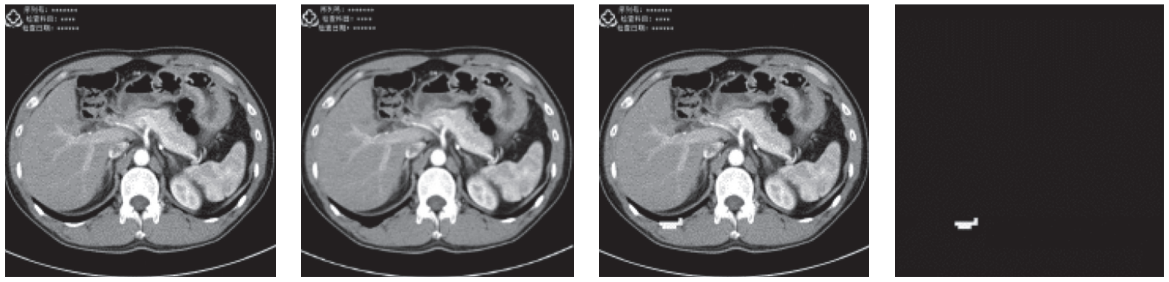
(a) (b) (c) (d)

Figure 15: Tamper localization effect on a skull image. (a) The skull image after embedding the watermark. (b) Tampered image. (c) Tamper localization image. (d) Position matrix of the tampered location.

marked in white. The algorithm can accurately locate the tampered area.

The watermarking embedding method is an important step to determine the robustness and transparency of the whole digital watermarking system. A good algorithm can not only guarantee the robustness but also improve the accuracy of image watermarking.

The accuracy of tamper detection is calculated by the following two aspects: (1) the positive detection rate (TPR), which is the ratio of the number of the correctly detected



(a) (b) (c) (d)

Figure 16: Tamper localization effect for a liver image. (a) The liver image after embedding the watermark. (b) Tampered image. (c) Tamper localization image. (d) Position matrix of the tampered location.

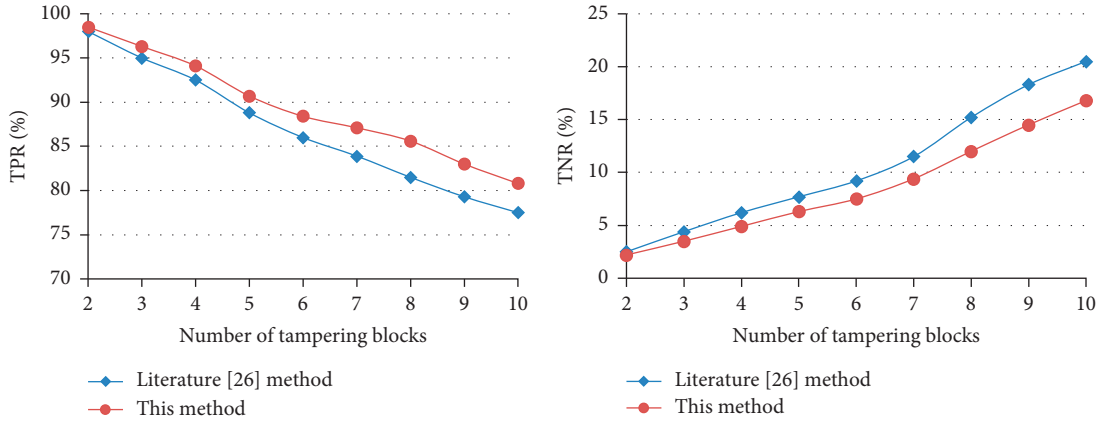


Figure 17: Comparison of the localization accuracy of the algorithm (40 experimental means). (a) Comparison of positive detection rate. (b) Comparison of negative detection rate.

tampering blocks to the total number of all the tampering blocks, and (2) the negative detection rate (TNR), which is the ratio of the number of the inaccurately detected tampering blocks to the total number of the tampered blocks.

Image tamper localization accuracy can be explained by the positive detection rate and negative detection rate. The pixel values of one or more pixel blocks of size 16×16 of the secret image are randomly selected. Figure 17(a) shows the mean of the positive detection rate after the 40 experiments; Figure 17(b) shows the mean value of the negative detection rate after the 40 experiments.

From Figure 17(a), we can know that, with the increase of tampered blocks, two methods of positive detection rate showed a downward trend; however, this method is obviously better than [26]; Figure 17(b) shows that the tampered blocks increases lead to a negative detection rate that showed an upward trend. This method rises slowly relative to the method in [26]. Of course, if tampering leads to information error of decomposition blocks, the negative detection rate will rise sharply. Based on the comprehensive analysis of the curve data in Figure 17 compared with the method of [26], the tamper localization accuracy of this method can be increased by almost 3%.

5. Conclusions

Because of the limitation of a single function in the existing medical image watermarking algorithms, a multipurpose watermarking algorithm for medical images is proposed in this paper. Theoretical analysis and experimental results show that the algorithm has good invisibility. In addition, the multiple watermarking algorithm achieves the multiple protection of the original medical image at the expense of minimal watermarking robustness. The ROI feature in medical images is used as an authentication watermark to enhance the sensitivity of tampering. At the same time, the generated feature authentication watermark is embedded not only in the medical image RONI but also in the corresponding ROI of other mapping blocks, which can effectively resist collage attacks and mean value attacks, enhance the tamper localization ability, and improve the positioning accuracy.

Image fusion theory is used to embed the visible watermark, which is equivalent to adding digital signatures to carrier images. Only when the digital signature (visible watermark) exists can the receiver extract the invisible watermark by using the key. Therefore, the multiple

watermarking algorithm is very suitable for copyright protection and declaration of important or sensitive data.

Data Availability

All relevant data are within the paper.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Statistical Science Research Project (2018LY12).

References

[1] M. Arsalan, A. S. Qureshi, A. Khan, and M. Rajarajan, "Protection of medical images and patient related information in healthcare: using an intelligent and reversible watermarking technique," *Applied Soft Computing*, vol. 51, pp. 168–179, 2017.

[2] P. Singh and S. Agarwal, "An efficient fragile watermarking scheme with multilevel tamper detection and recovery based on dynamic domain selection," *Multimedia Tools and Applications*, vol. 75, no. 14, pp. 8165–8194, 2016.

[3] N. A. Memon and A. Alzahrani, "Prediction-based reversible watermarking of CT scan images for content authentication and copyright protection," *IEEE Access*, vol. 8, pp. 75448–75462, 2020.

[4] Z. Zhang, L. Wu, H. Lai et al., "Double reversible watermarking algorithm for image tamper detection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 3, pp. 530–542, 2016.

[5] W. Berchtold, M. Schäfer, S. Wombacher, and M. Steinebach, "Quality metric for 2D textures on 3D objects," *Electronic Imaging*, vol. 2016, no. 8, pp. 1–6, 2016.

[6] A. K. Singh, M. Dave, and A. Mohan, "Hybrid technique for robust and imperceptible multiple watermarking using medical images," *Multimedia Tools and Applications*, vol. 75, no. 14, pp. 8381–8401, 2016.

[7] J. Liu, J. Li, J. Ma, N. Sadiq, U. Bhatti, and Y. Ai, "A robust multi-watermarking algorithm for medical images based on DTCWT-DCT and henon map," *Applied Sciences*, vol. 9, no. 4, pp. 700–722, 2019.

[8] T. Ye, "A self-embedding image watermarking scheme with dual purpose," *Acta Photonica Sinica*, vol. 41, no. 7, pp. 859–866, 2012.

[9] W. Li, L. Gao, X. Kong et al., "A blind watermark algorithm for medical images using ROI and contourlet," *Journal of Harbin Engineering University*, vol. 34, no. 7, pp. 918–923, 2013.

[10] L.-L. Tang, C. T. Huang, J.-S. Pan, and C.-Y. Liu, "Dual watermarking algorithm based on the fractional fourier transform," *Multimedia Tools and Applications*, vol. 74, no. 12, pp. 4397–4413, 2013.

[11] H. Shi, M.-C. Li, C. Guo, and R. Tan, "A region-adaptive semi-fragile dual watermarking scheme," *Multimedia Tools and Applications*, vol. 75, no. 1, pp. 465–495, 2016.

[12] A. Shehab, M. Elhoseny, K. Muhammad et al., "Secure and robust fragile watermarking scheme for medical images," *IEEE Access*, vol. 6, pp. 10269–10278, 2018.

[13] B. Lei, X. Zhao, H. Lei et al., "Multipurpose watermarking scheme via intelligent method and chaotic map," *Multimedia Tools & Applications*, vol. 78, no. 19, pp. 27085–27107, 2017.

[14] N. N. Hurrah, S. A. Parah, N. A. Loan, J. A. Sheikh, M. Elhoseny, and K. Muhammad, "Dual watermarking framework for privacy protection and content authentication of multimedia," *Future Generation Computer Systems*, vol. 94, no. 5, pp. 654–673, 2019.

[15] K. Swaraja, K. Meenakshi, and K. Padmavathi, "An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine," *Biomedical Signal Processing and Control*, vol. 55, Article ID 101665, 2019.

[16] X. Gong, L. Chen, F. Yu, X. Zhao, and S. Wang, "A secure image authentication scheme based on dual fragile watermark," *Multimedia Tools and Applications*, vol. 79, no. 25-26, pp. 18071–18088, 2020.

[17] R. Thanki, S. Borra, V. Dwivedi et al., "A RONI based visible watermarking approach for medical image authentication," *Journal of Medical Systems*, vol. 41, no. 9, pp. 143–153, 2017.

[18] B. Feng, X. Li, Y. Jie, C. Guo, and H. Fu, "A novel semi-fragile digital watermarking scheme for scrambled image authentication and restoration," *Mobile Networks and Applications*, vol. 25, no. 1, pp. 82–94, 2020.

[19] Z. Qiang, L. He, Y. Chen, X. Chen, and D. Xu, "Adaptive fast local Laplacian filters and its edge-aware application," *Multimedia Tools and Applications*, vol. 78, no. 1, pp. 619–639, 2019.

[20] P. Fan, R.-G. Zhou, W. W. Hu, and N. Jing, "Quantum image edge extraction based on Laplacian operator and zero-cross method," *Quantum Information Processing*, vol. 18, no. 1, pp. 1–23, 2019.

[21] S. Osher and J. Sethian, "Fronts propagating with curvature dependent speed: algorithms based the Hamilton Jacobi formulation," *Journal of Computational Physics*, vol. 79, no. 1, pp. 12–49, 1998.

[22] F. Zhang, X. Zhang, and D. Shang, "Digital watermarking algorithm based on Kalman filtering and image fusion," *Neural Computing and Applications*, vol. 21, no. 6, pp. 1149–1157, 2012.

[23] P. Pandey, S. Kumar, and S. K. Singh, "Rightful ownership through image adaptive DWT-SVD watermarking algorithm and perceptual tweaking," *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 723–748, 2014.

[24] S. S. Yadav and Y. Singh, "Image encryption based on random scrambling and chaotic logistic map," *International Journal of Grid and Utility Computing*, vol. 9, no. 3, pp. 228–234, 2018.

[25] Z. Zhang, L. Wu, Y. Yan et al., "Adaptive reversible image watermarking algorithm based on DE," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 3, pp. 1761–1784, 2017.

[26] P. Singh and S. Agarwal, "A self recoverable dual watermarking scheme for copyright protection and integrity verification," *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6389–6428, 2017.

[27] K.-C. Choi and C.-M. Pun, "Robust lossless digital watermarking using integer transform with bit plane manipulation," *Multimedia Tools and Applications*, vol. 75, no. 11, pp. 6621–6645, 2016.

[28] R. Thanki and S. Borra, "Fragile watermarking for copyright authentication and tamper detection of medical images using compressive sensing (CS) based encryption and contourlet domain processing," *Multimedia Tools and Applications*, vol. 78, no. 10, pp. 13905–13924, 2019.